FIG. 1

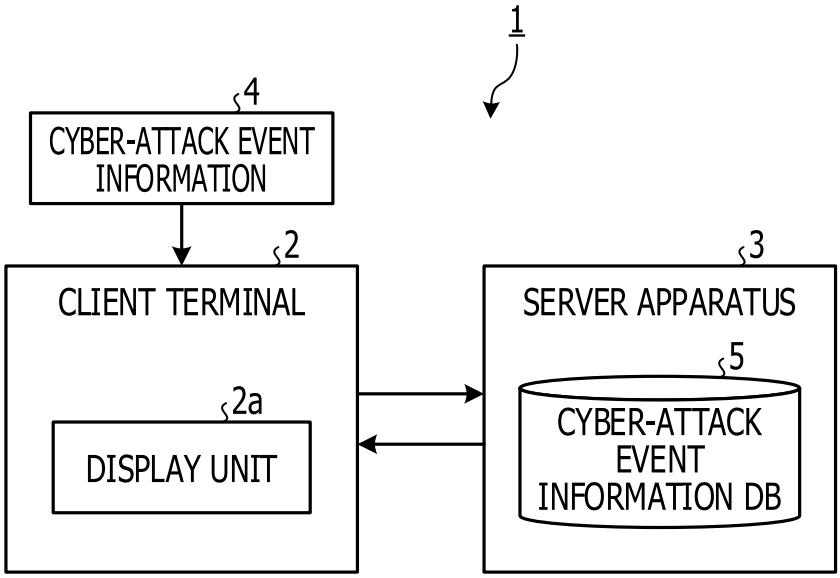

1
4
CYBER-ATTACK EVENT INFORMATION
2
CLIENT TERMINAL
2a
DISPLAY UNIT
3
SERVER APPARATUS
5
CYBER-ATTACK EVENT INFORMATION DB

FIG. 2

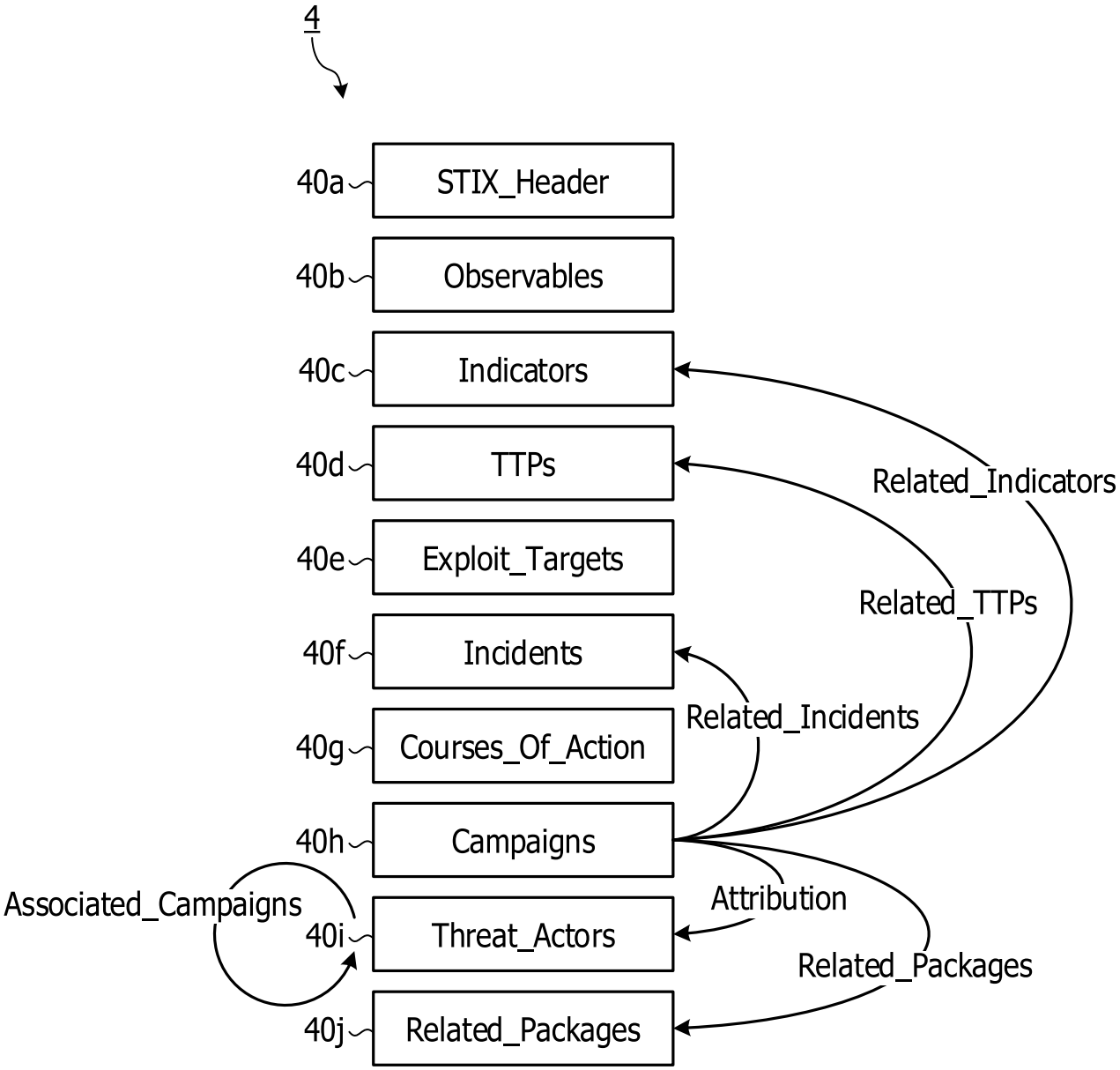

4
40a
STIX_Header
40b
Observables
40c
Indicators
40d
TTPs
40e
Exploit_Targets
40f
Incidents
40g
Courses_Of_Action
40h
Campaigns
40i
Threat_Actors
40j
Related_Packages
Related_Indicators
Related_TTPs
Related_Incidents
Attribution
Related_Packages
Associated_Campaigns

FIG. 3

4

```
        ⋮

<!-- CYBER-ATTACK ACTIVITY -->
<stix:Campaigns>
<stix:Campaign xsi:type="campaign:CampaignType" id="IPA:campaign_example">
<campaign:Title>TITLE RELATING TO CYBER-ATTACK ACTIVITY</campaign:Title>
<campaign:Description>DESCRIPTION OF CYBER-ATTACK ACTIVITY</campaign:Description>
<campaign:Short_Description>OUTLINE OF CYBER-ATTACK ACTIVITY</campaign:Short_Description>
<campaign:Names>
<campaign:Name>NAME OF CYBER-ATTACK ACTIVITY</campaign:Name>
</campaign:Names>
<!-- INTENTION OF ATTACK ACTIVITY -->
<campaign:Intended_Effect>
<stixCommon:Value xsi:type="stixVocabs:IntendedEffectVocab-1.0">Unauthorized Access</
stixCommon:Value>
</campaign:Intended_Effect>
<!-- STATE OF ATTACK ACTIVITY -->
<campaign:Status xsi:type="stixVocabs:CampaignStatusVocab-1.0">Historic</campaign:Status>
<!-- ATTACK METHOD RELATING TO ATTACK ACTIVITY -->
<campaign:Related_TTPs>
<campaign:Related_TTP>
<stixCommon:TTP idref="IPA:ttp_example"/>
</campaign:Related_TTP>
</campaign:Related_TTPs>
<!-- INCIDENT RELATING TO ATTACK ACTIVITY -->
<campaign:Related_Incidents>
<campaign:Related_Incident>
<stixCommon:Incident idref="IPA:incident_example"/>
</campaign:Related_Incident>
</campaign:Related_Incidents>
        ⋮
```

FIG. 4

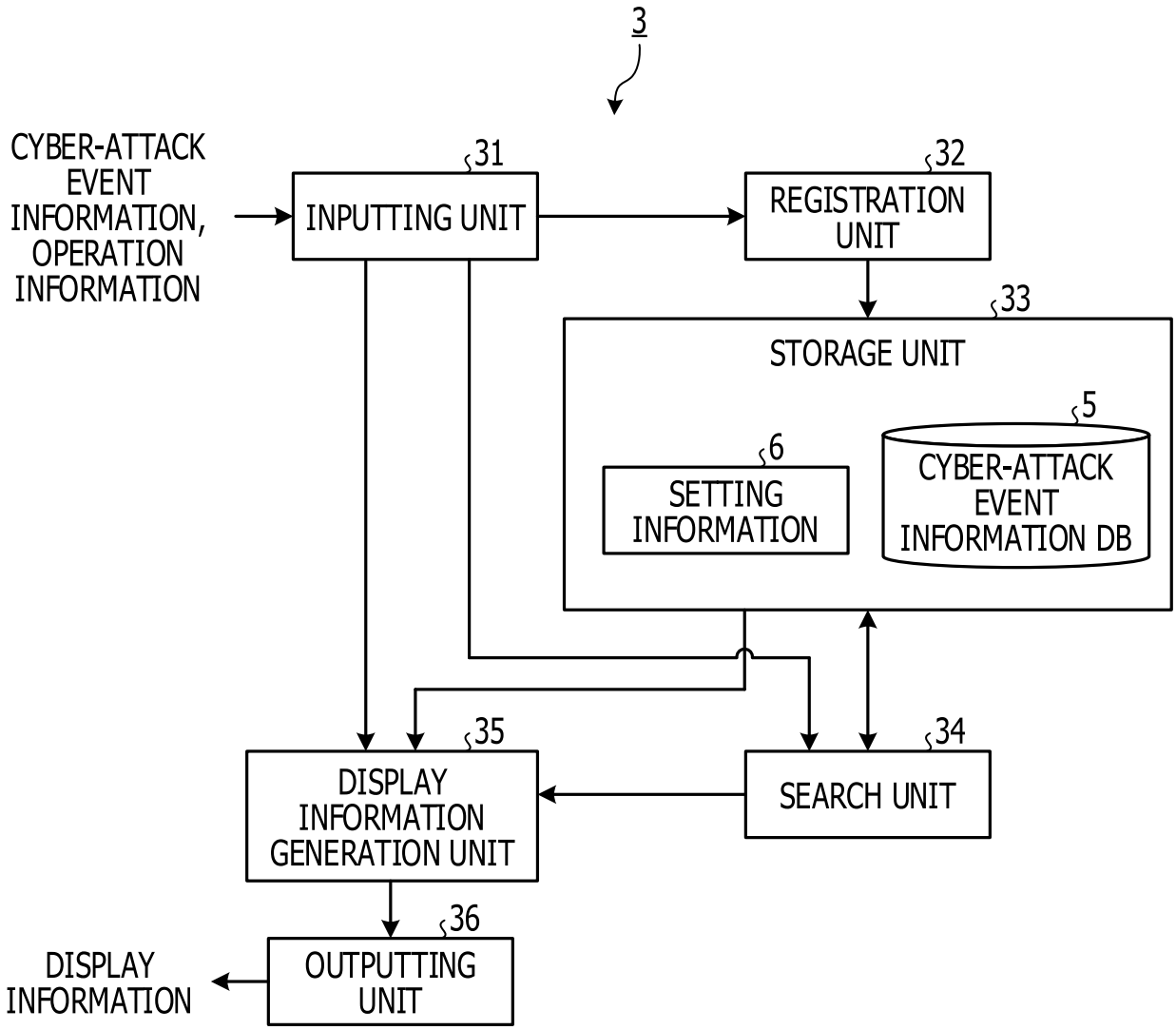

3
CYBER-ATTACK EVENT INFORMATION, OPERATION INFORMATION
31
INPUTTING UNIT
32
REGISTRATION UNIT
33
STORAGE UNIT
5
6
SETTING INFORMATION
CYBER-ATTACK EVENT INFORMATION DB
35
DISPLAY INFORMATION GENERATION UNIT
34
SEARCH UNIT
36
OUTPUTTING UNIT
DISPLAY INFORMATION

FIG. 5

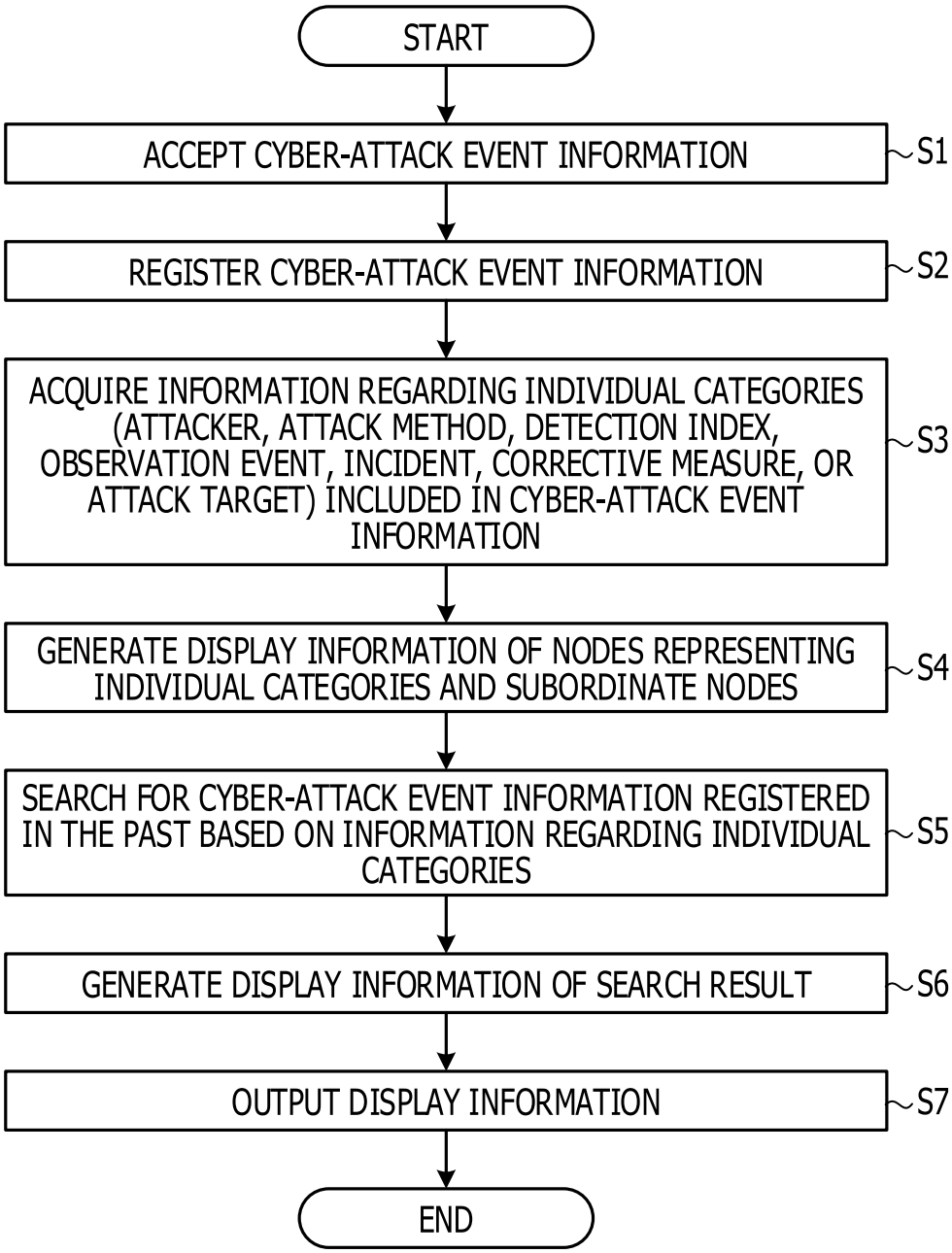

START
ACCEPT CYBER-ATTACK EVENT INFORMATION
S1
REGISTER CYBER-ATTACK EVENT INFORMATION
S2
ACQUIRE INFORMATION REGARDING INDIVIDUAL CATEGORIES (ATTACKER, ATTACK METHOD, DETECTION INDEX, OBSERVATION EVENT, INCIDENT, CORRECTIVE MEASURE, OR ATTACK TARGET) INCLUDED IN CYBER-ATTACK EVENT INFORMATION
S3
GENERATE DISPLAY INFORMATION OF NODES REPRESENTING INDIVIDUAL CATEGORIES AND SUBORDINATE NODES
S4
SEARCH FOR CYBER-ATTACK EVENT INFORMATION REGISTERED IN THE PAST BASED ON INFORMATION REGARDING INDIVIDUAL CATEGORIES
S5
GENERATE DISPLAY INFORMATION OF SEARCH RESULT
S6
OUTPUT DISPLAY INFORMATION
S7
END

FIG. 6

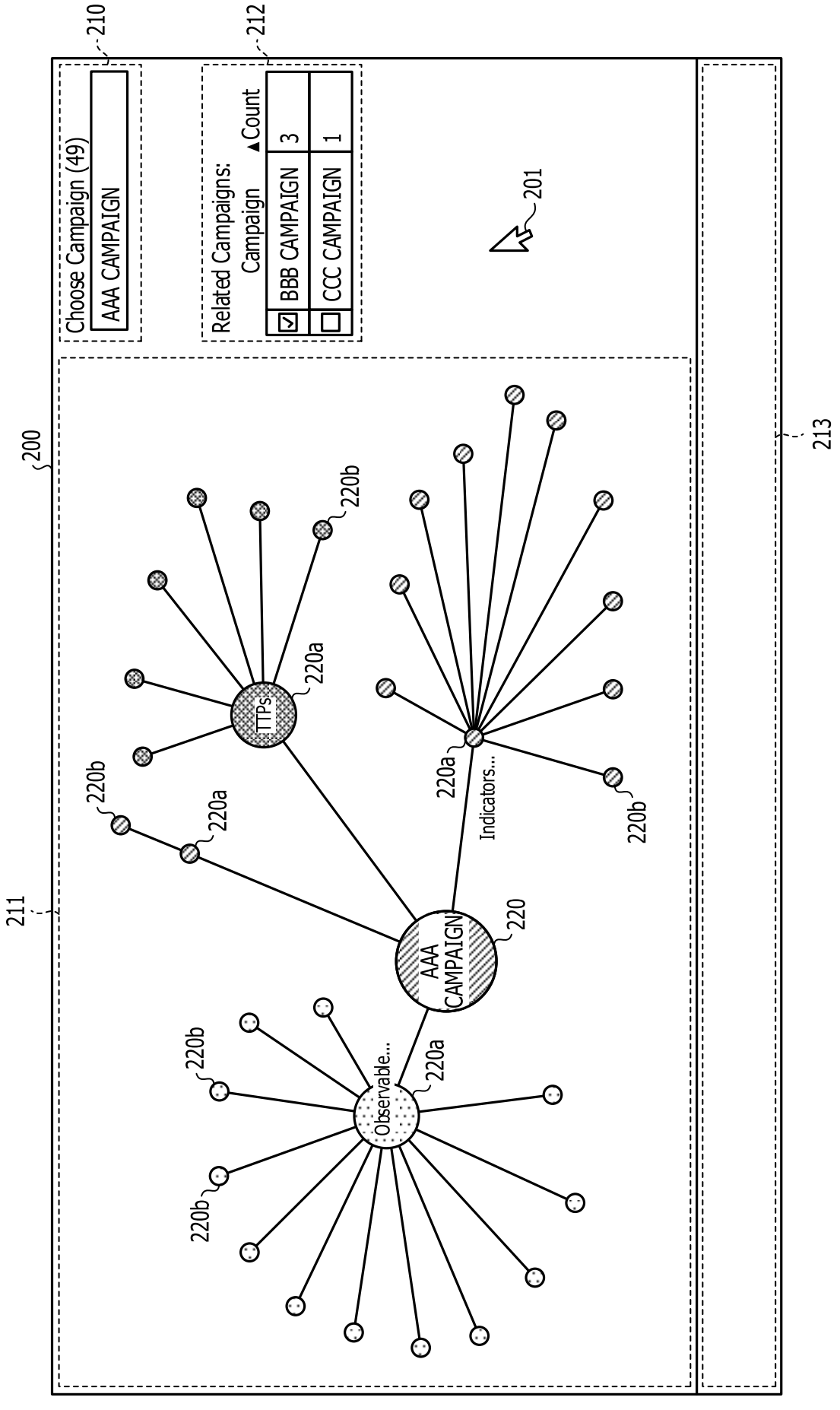

210
212
Choose Campaign (49)
AAA CAMPAIGN
Related Campaigns:
Campaign
Count
BBB CAMPAIGN
3
CCC CAMPAIGN
1
201
200
211
213
220b
220a
TTPs
220a
220b
220b
220a
Indicators...
220b
AAA CAMPAIGN
220
220b
Observable...
220a
220b

FIG. 7

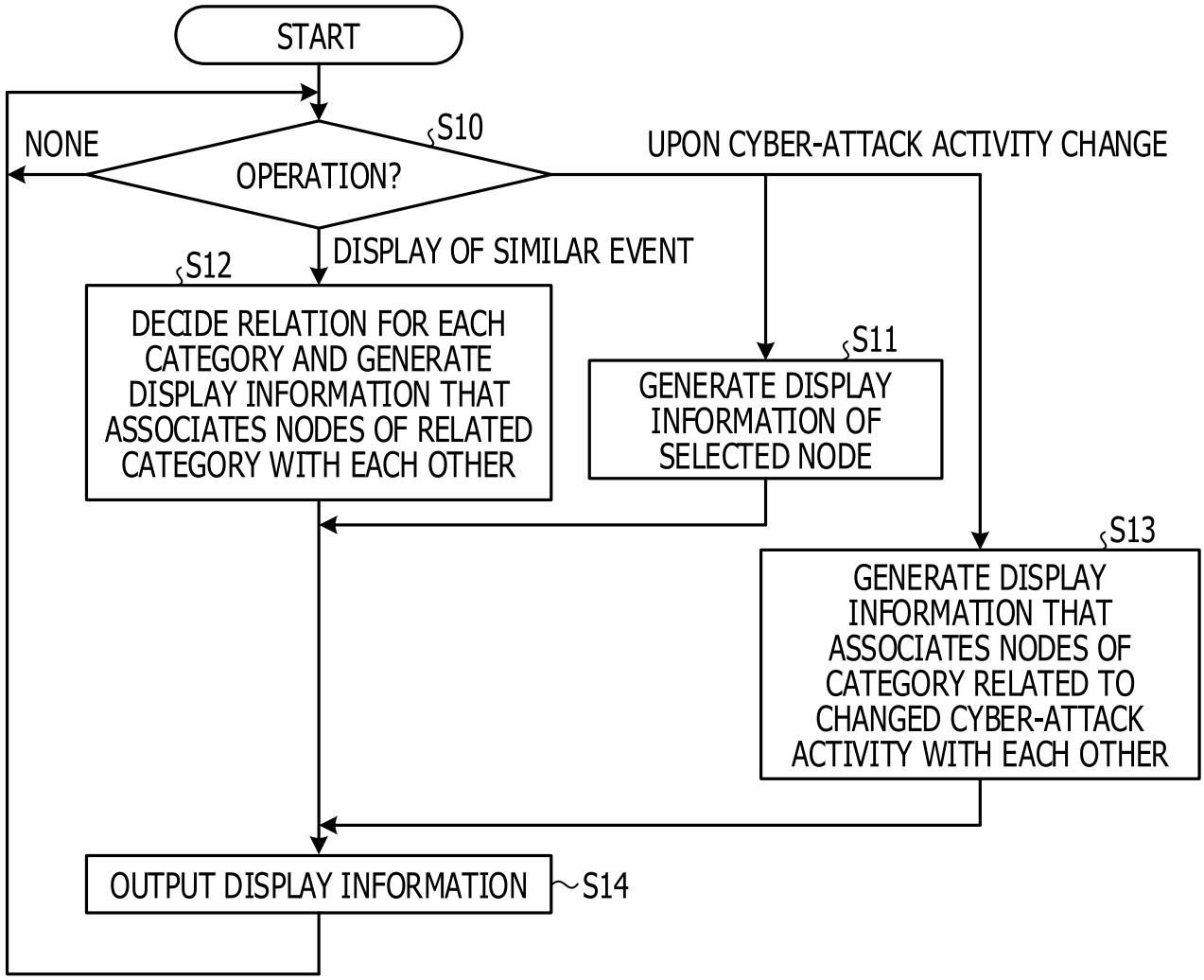

START
S10
OPERATION?
NONE
UPON CYBER-ATTACK ACTIVITY CHANGE
DISPLAY OF SIMILAR EVENT
S12
DECIDE RELATION FOR EACH CATEGORY AND GENERATE DISPLAY INFORMATION THAT ASSOCIATES NODES OF RELATED CATEGORY WITH EACH OTHER
S11
GENERATE DISPLAY INFORMATION OF SELECTED NODE
S13
GENERATE DISPLAY INFORMATION THAT ASSOCIATES NODES OF CATEGORY RELATED TO CHANGED CYBER-ATTACK ACTIVITY WITH EACH OTHER
OUTPUT DISPLAY INFORMATION
S14

FIG. 8

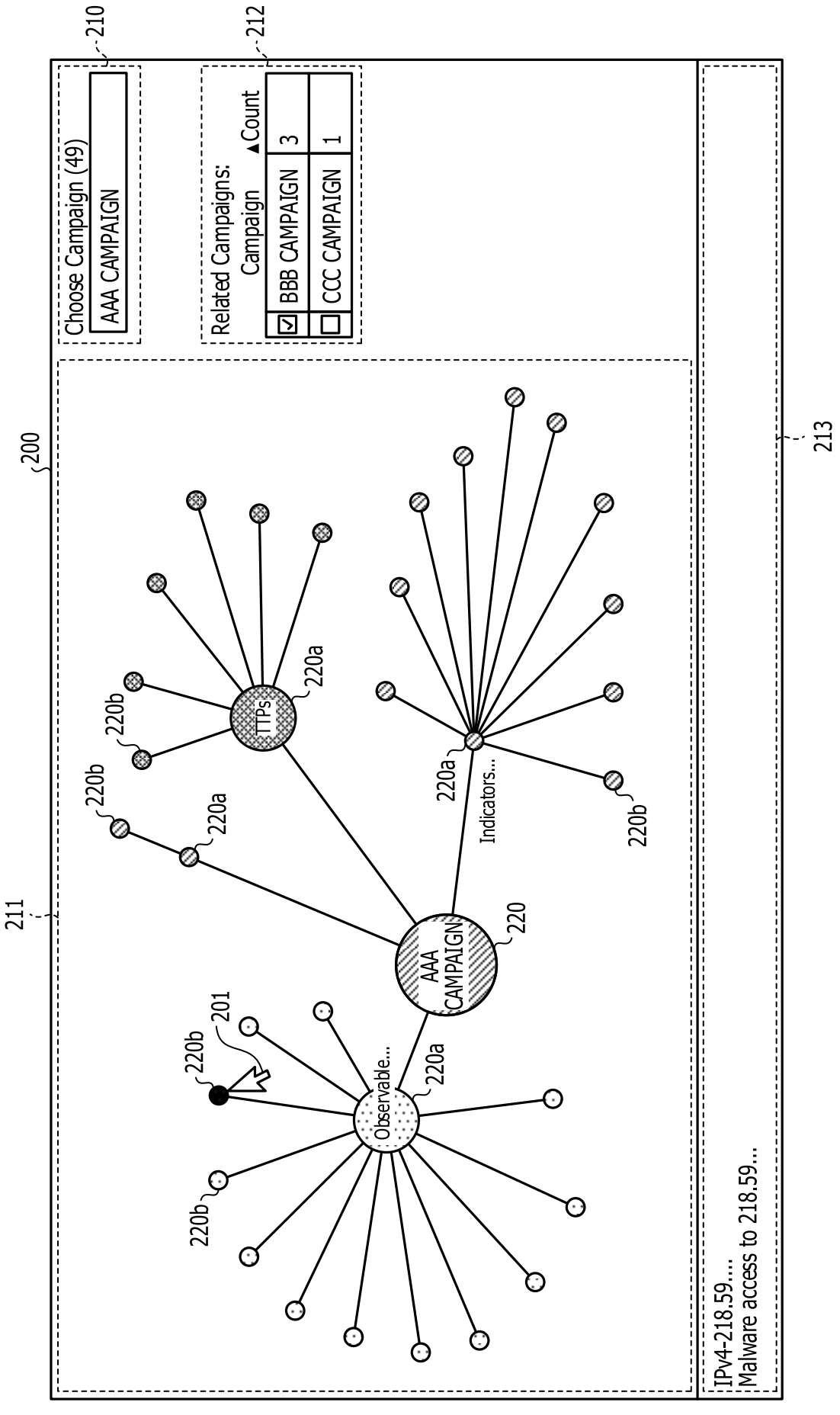

210
212
Choose Campaign (49)
AAA CAMPAIGN
Related Campaigns:
Campaign
Count
BBB CAMPAIGN
3
CCC CAMPAIGN
1
200
211
213
TTPs
220a
220b
Indicators...
AAA CAMPAIGN
220
Observable...
201
IPv4-218.59....
Malware access to 218.59...

FIG. 9

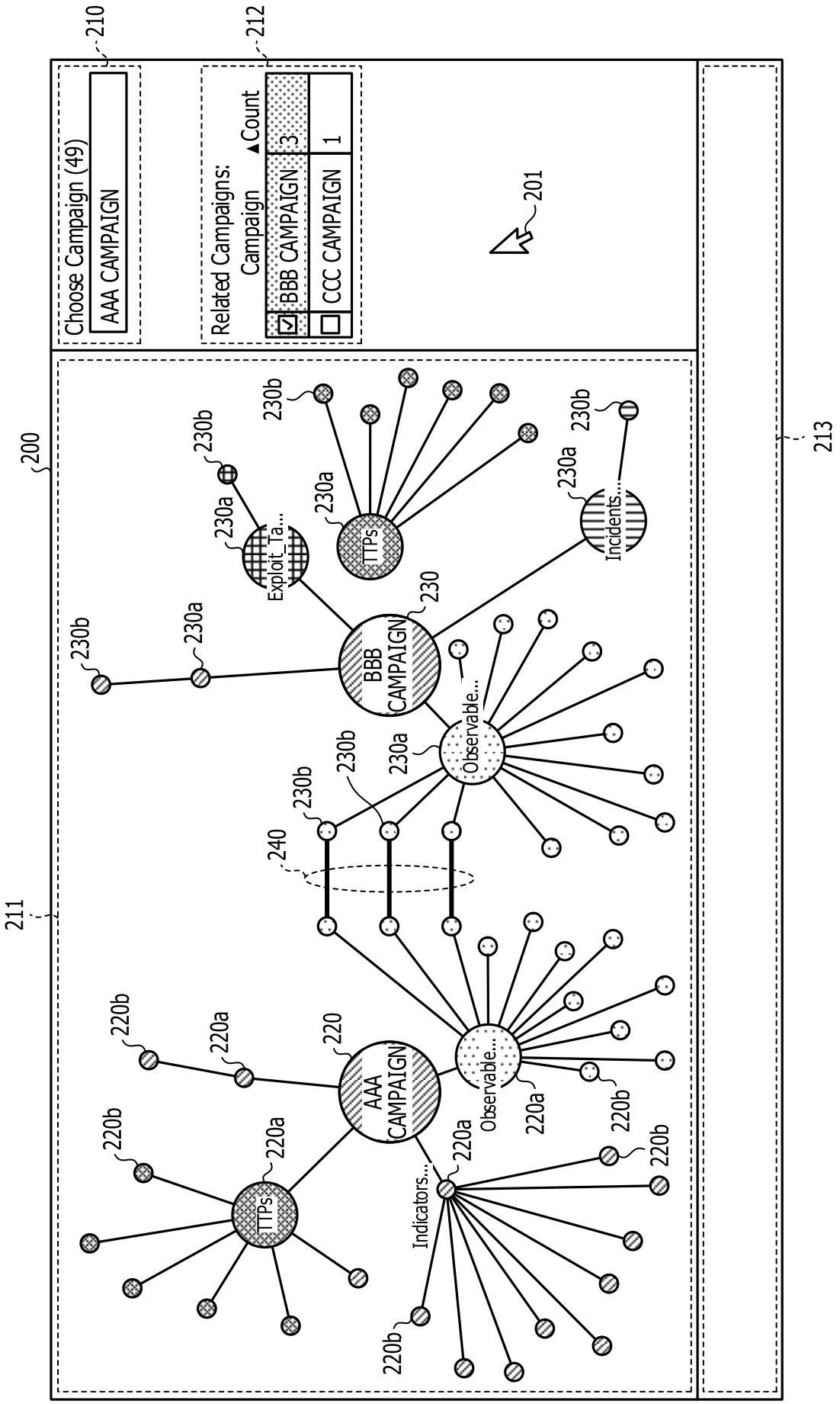
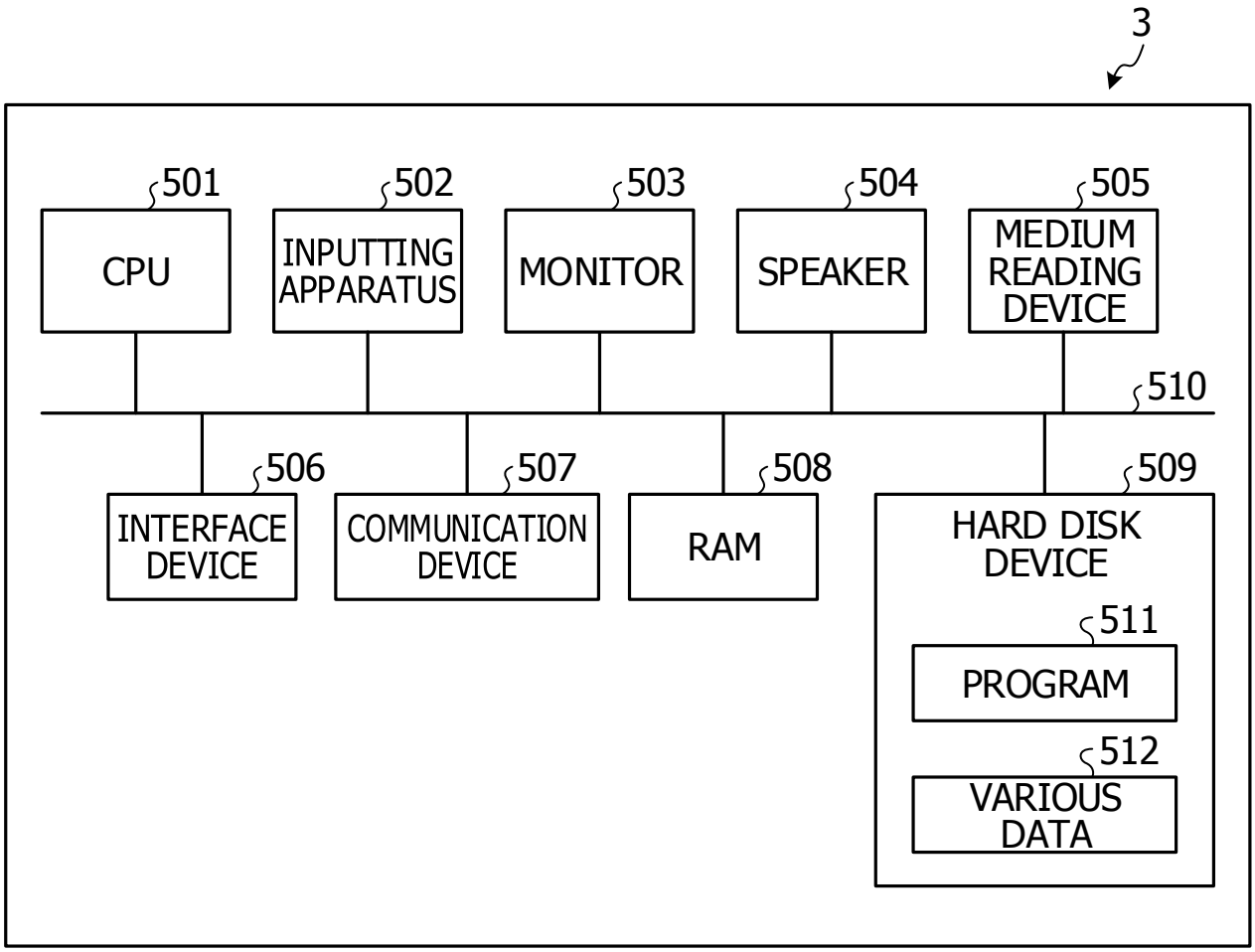

210
212
Choose Campaign (49)
AAA CAMPAIGN
Related Campaigns:
Campaign
Count
BBB CAMPAIGN 3
CCC CAMPAIGN 1
201
200
211
213
AAA CAMPAIGN
BBB CAMPAIGN
TTPs
Indicators...
Observable...
Exploit_Ta...
Incidents...
220
220a
220b
230
230a
230b
240

FIG. 10


3
501
CPU
502
INPUTTING APPARATUS
503
MONITOR
504
SPEAKER
505
MEDIUM READING DEVICE
510
506
INTERFACE DEVICE
507
COMMUNICATION DEVICE
508
RAM
509
HARD DISK DEVICE
511
PROGRAM
512
VARIOUS DATA