

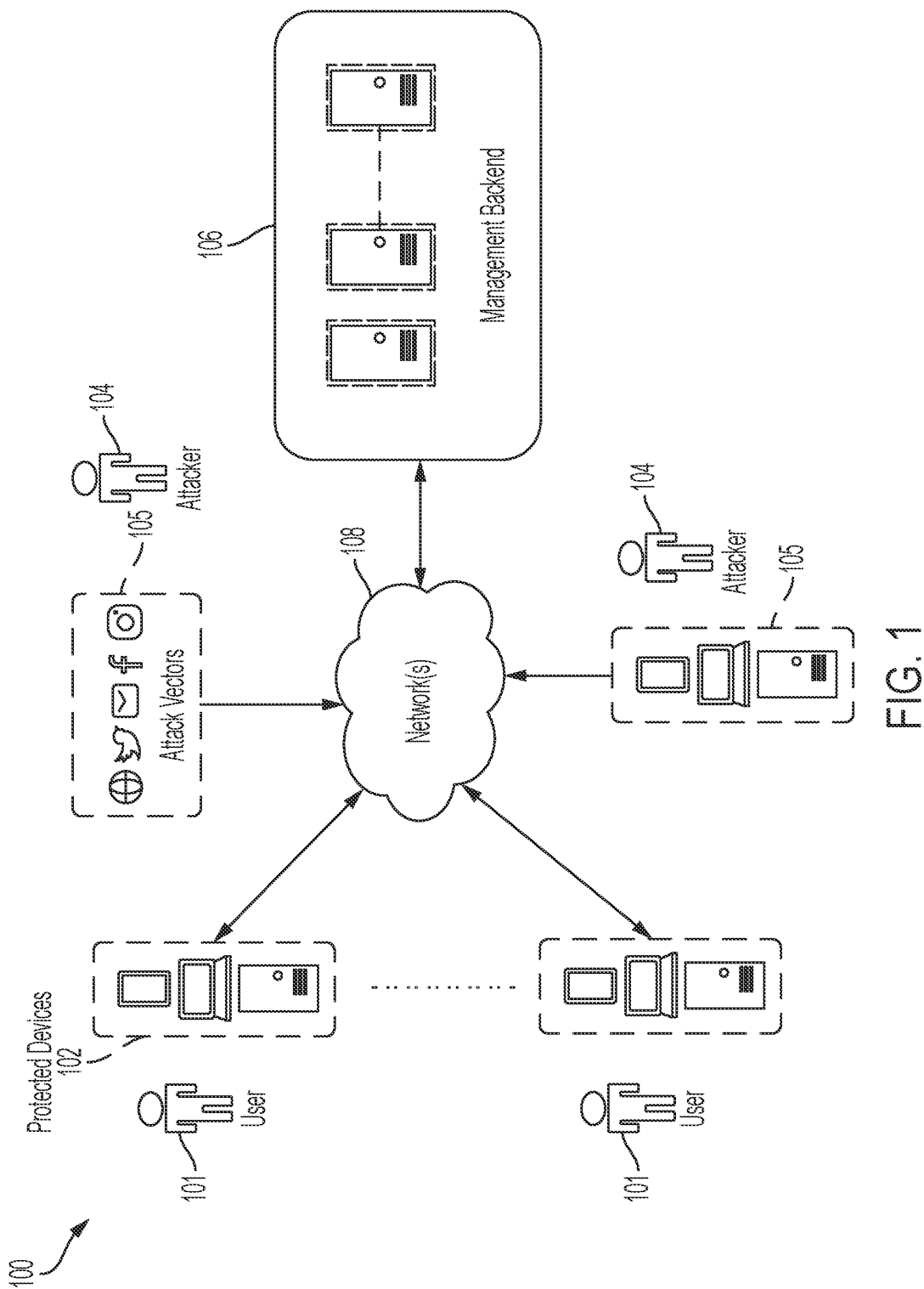


FIG. 1

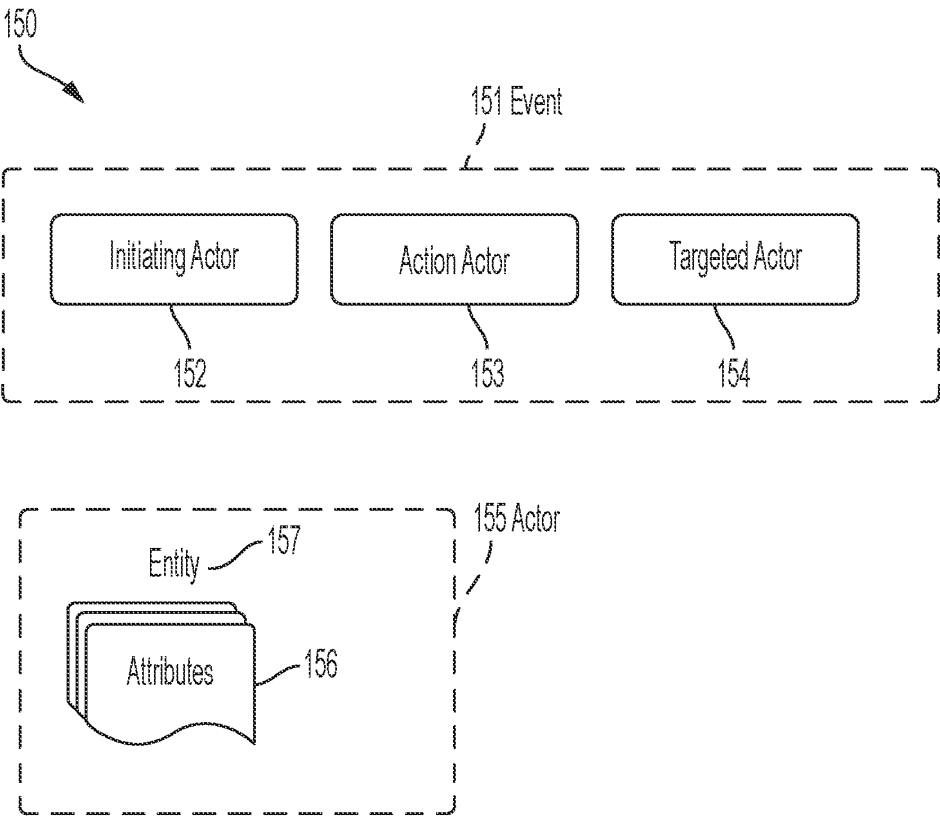


FIG. 2A

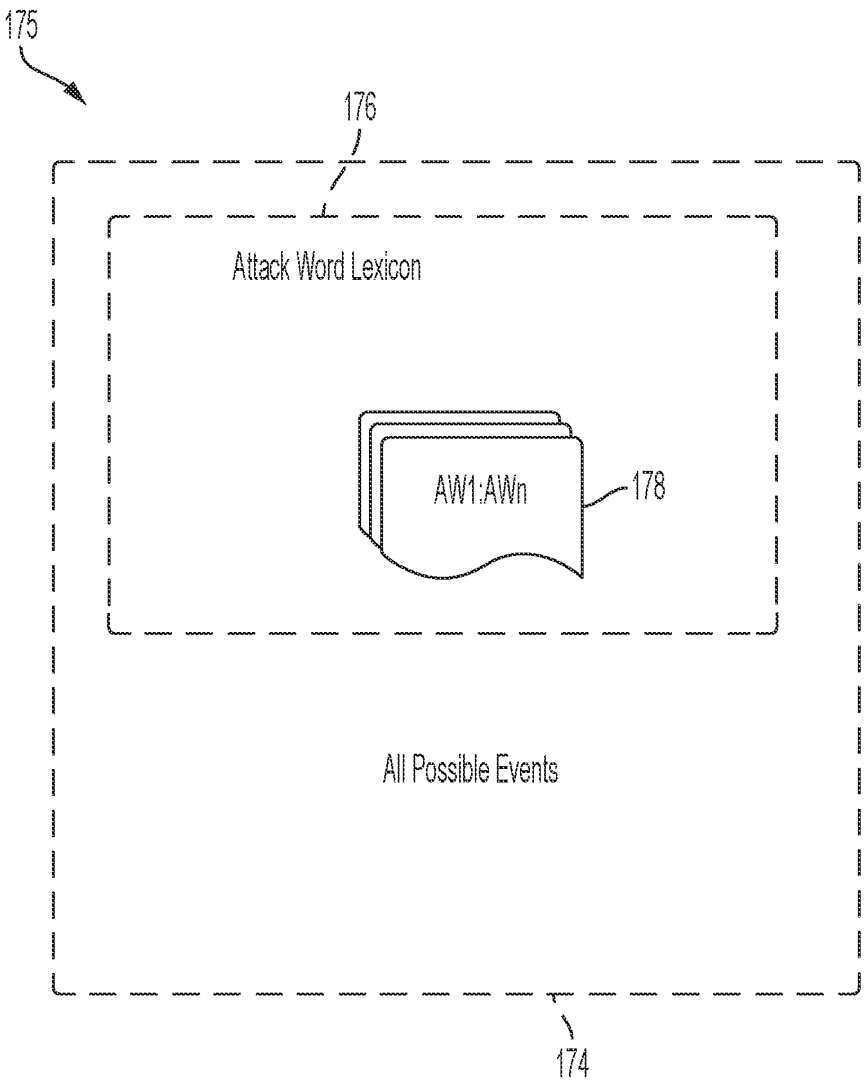


FIG. 2B

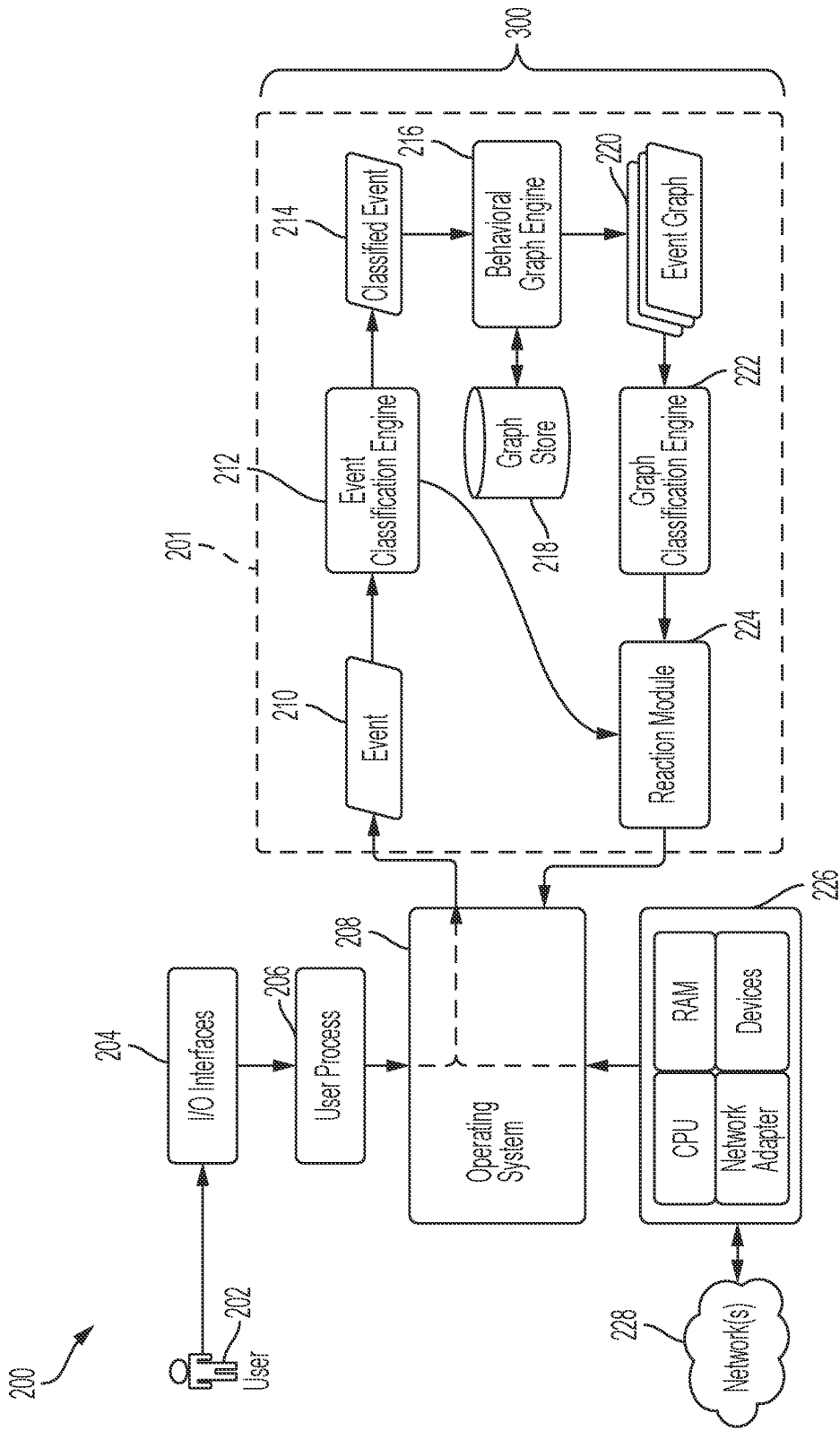


FIG. 3

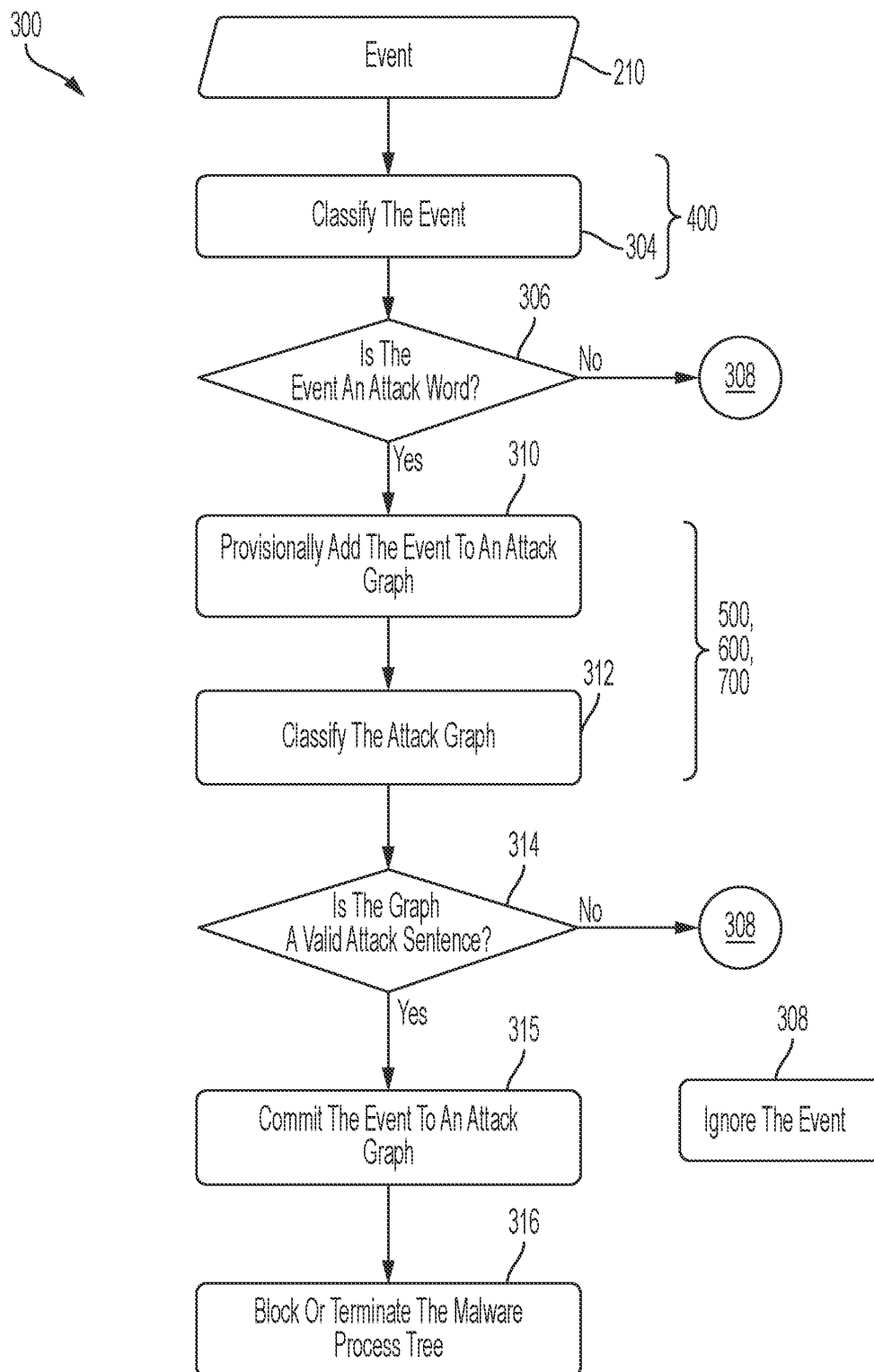


FIG. 4

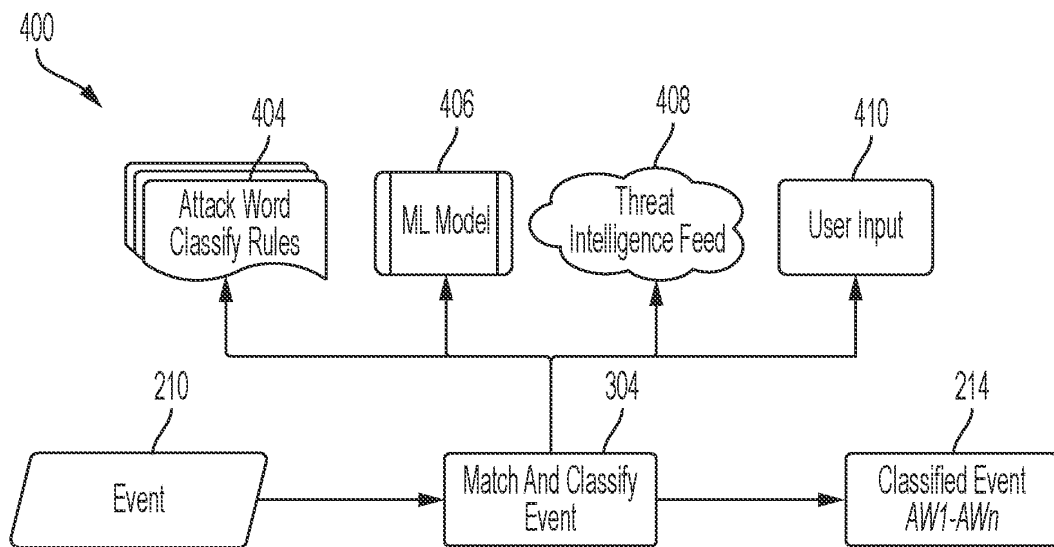


FIG. 5

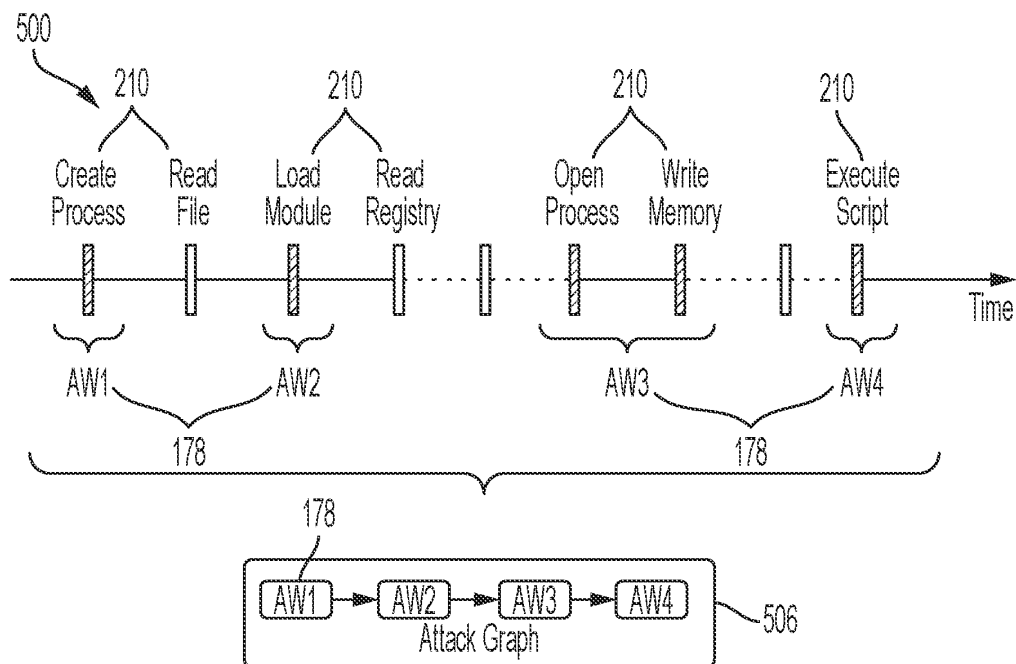


FIG. 6

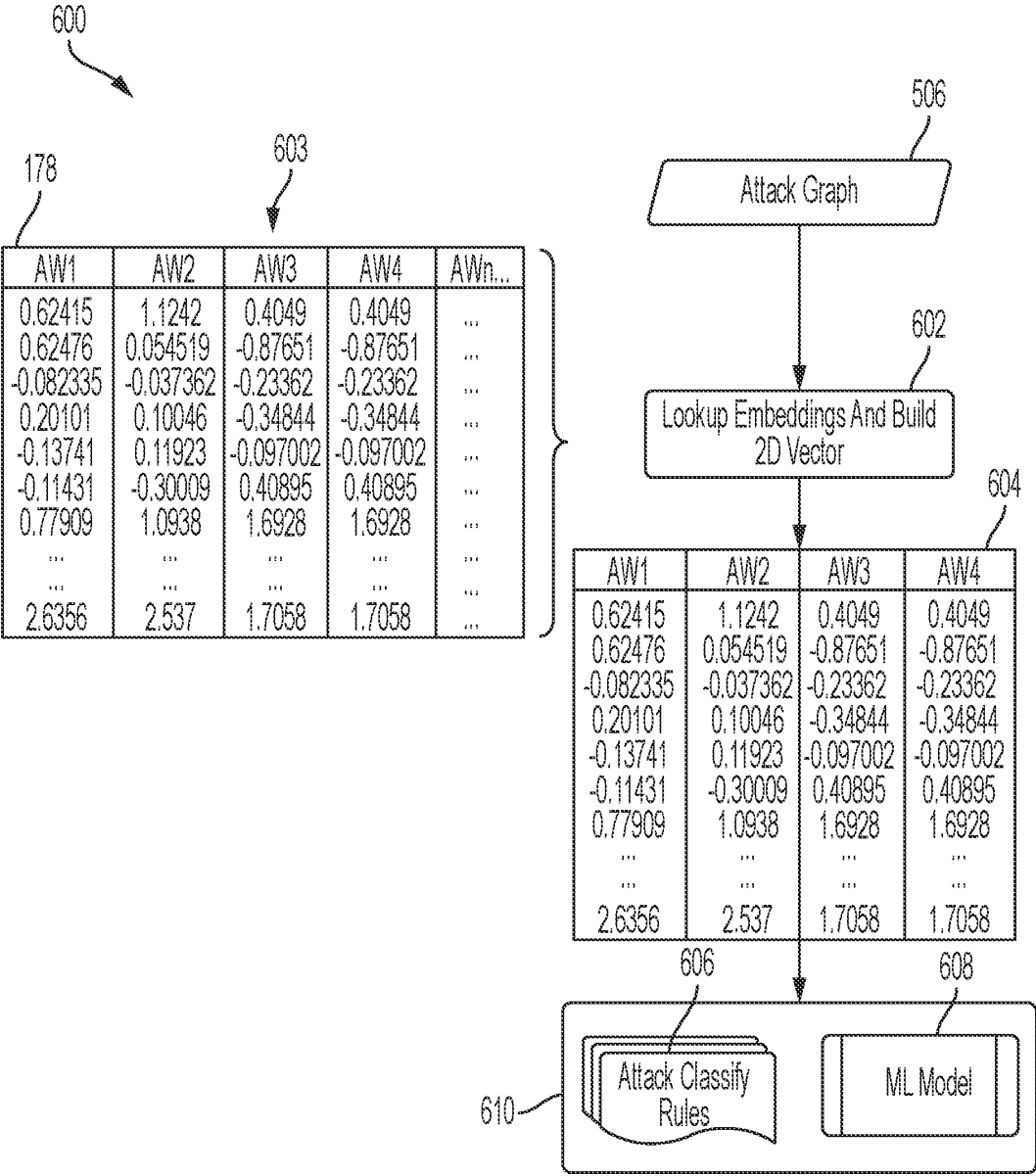


FIG. 7

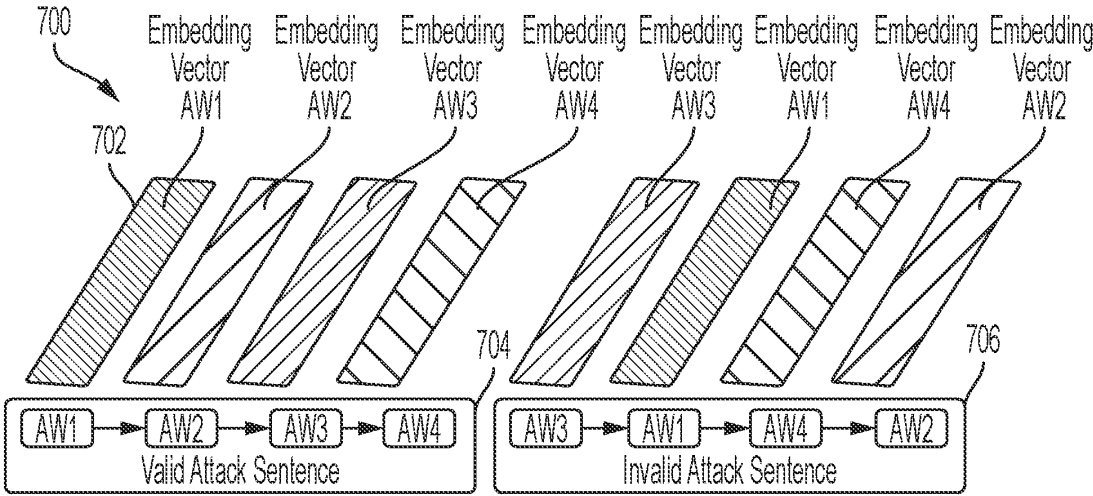


FIG. 8

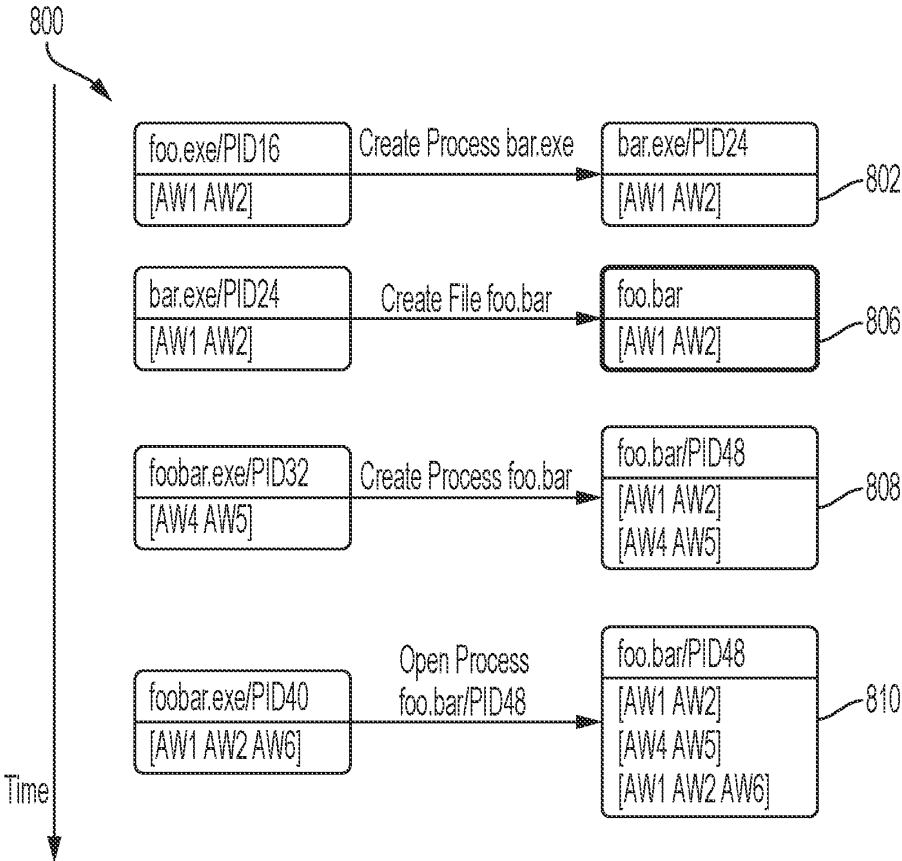


FIG. 9

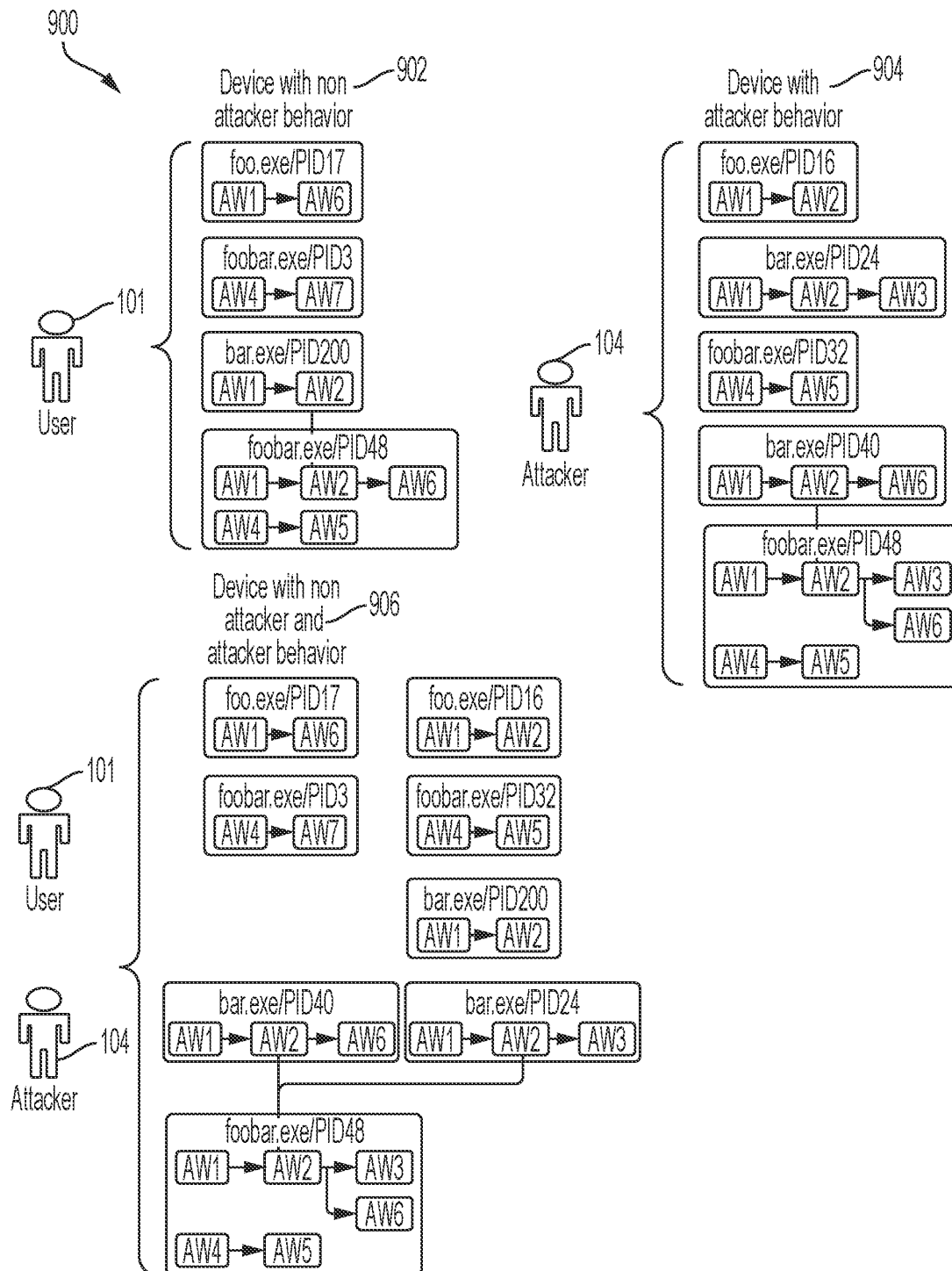
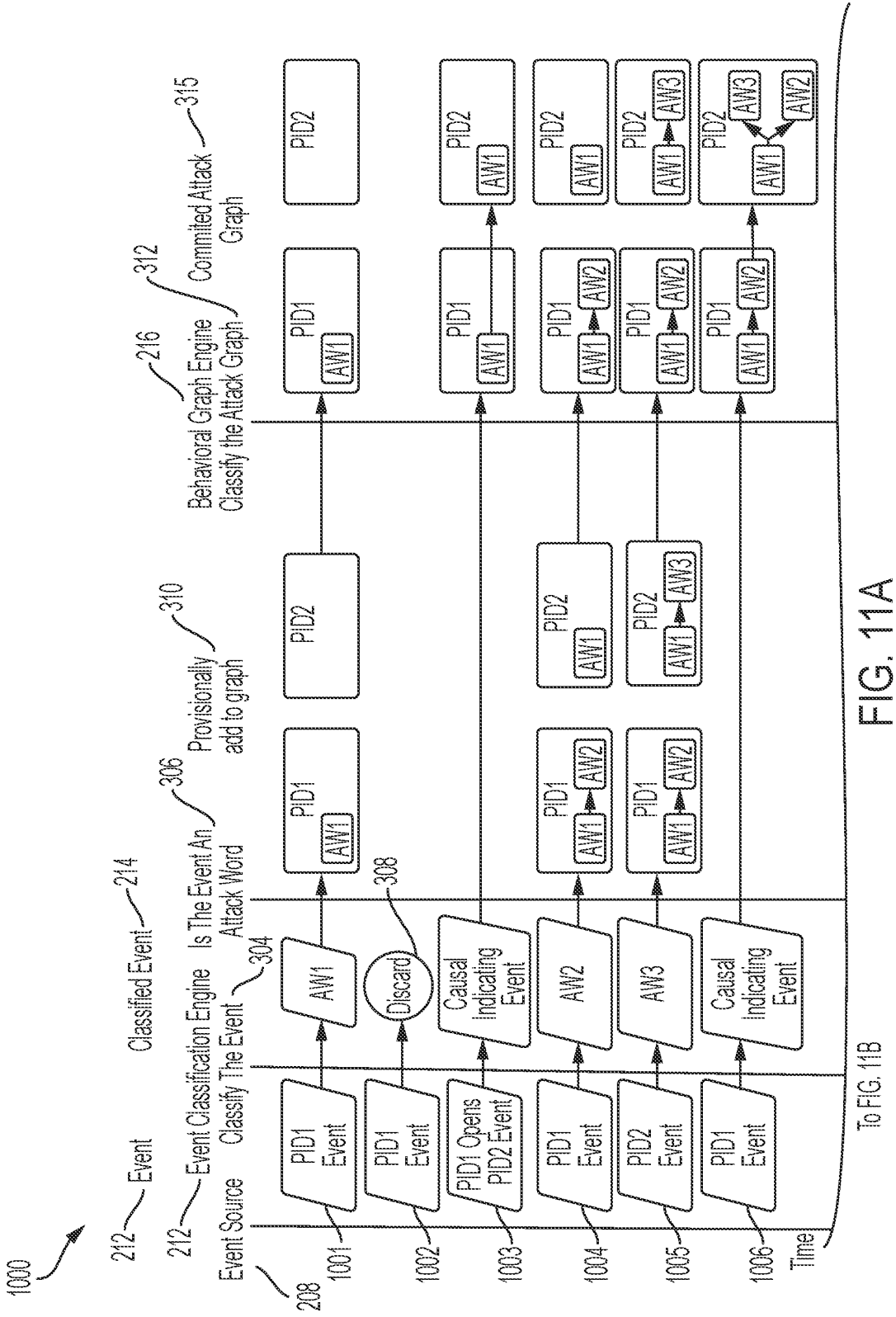


FIG. 10



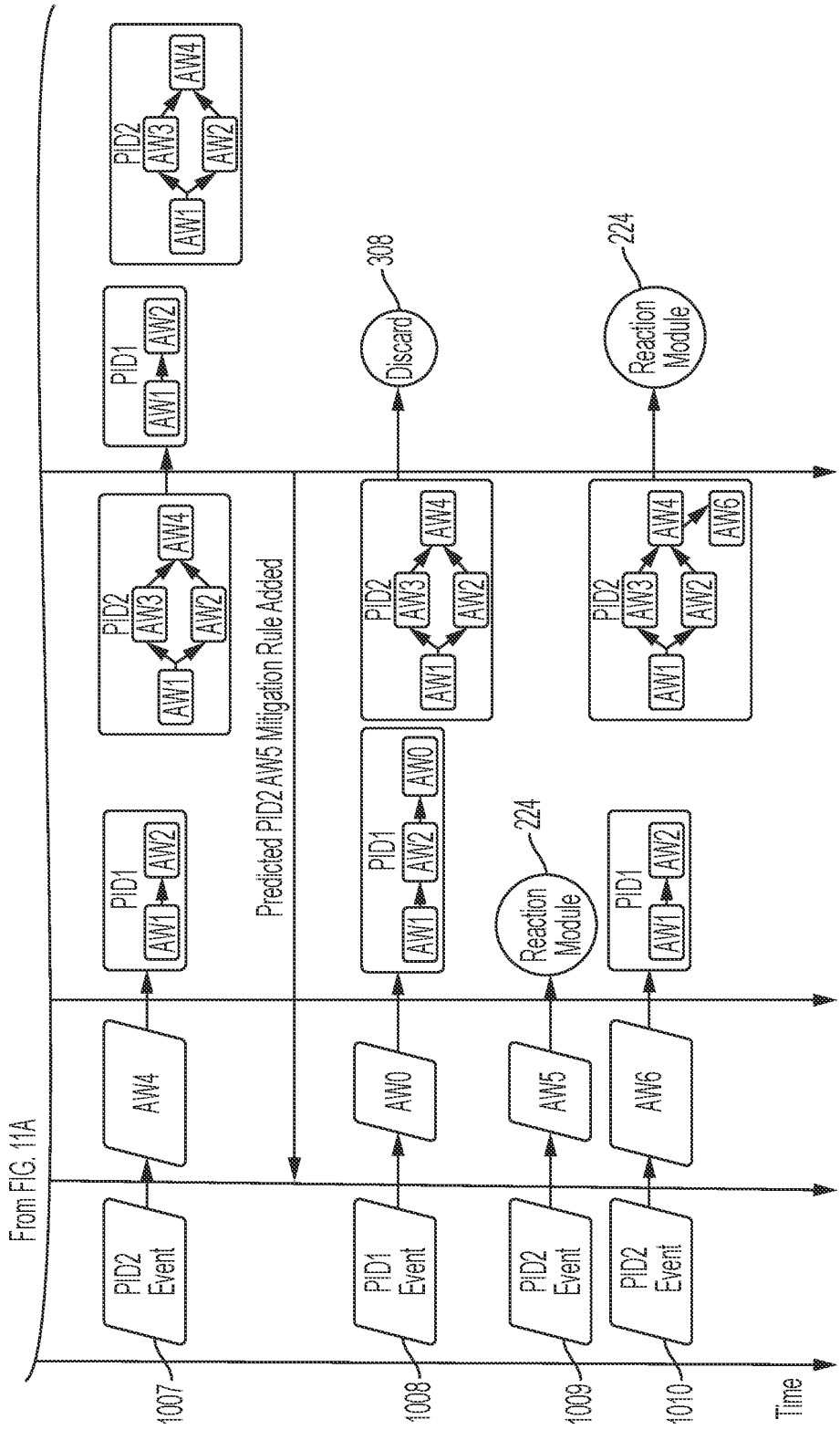


FIG. 11B

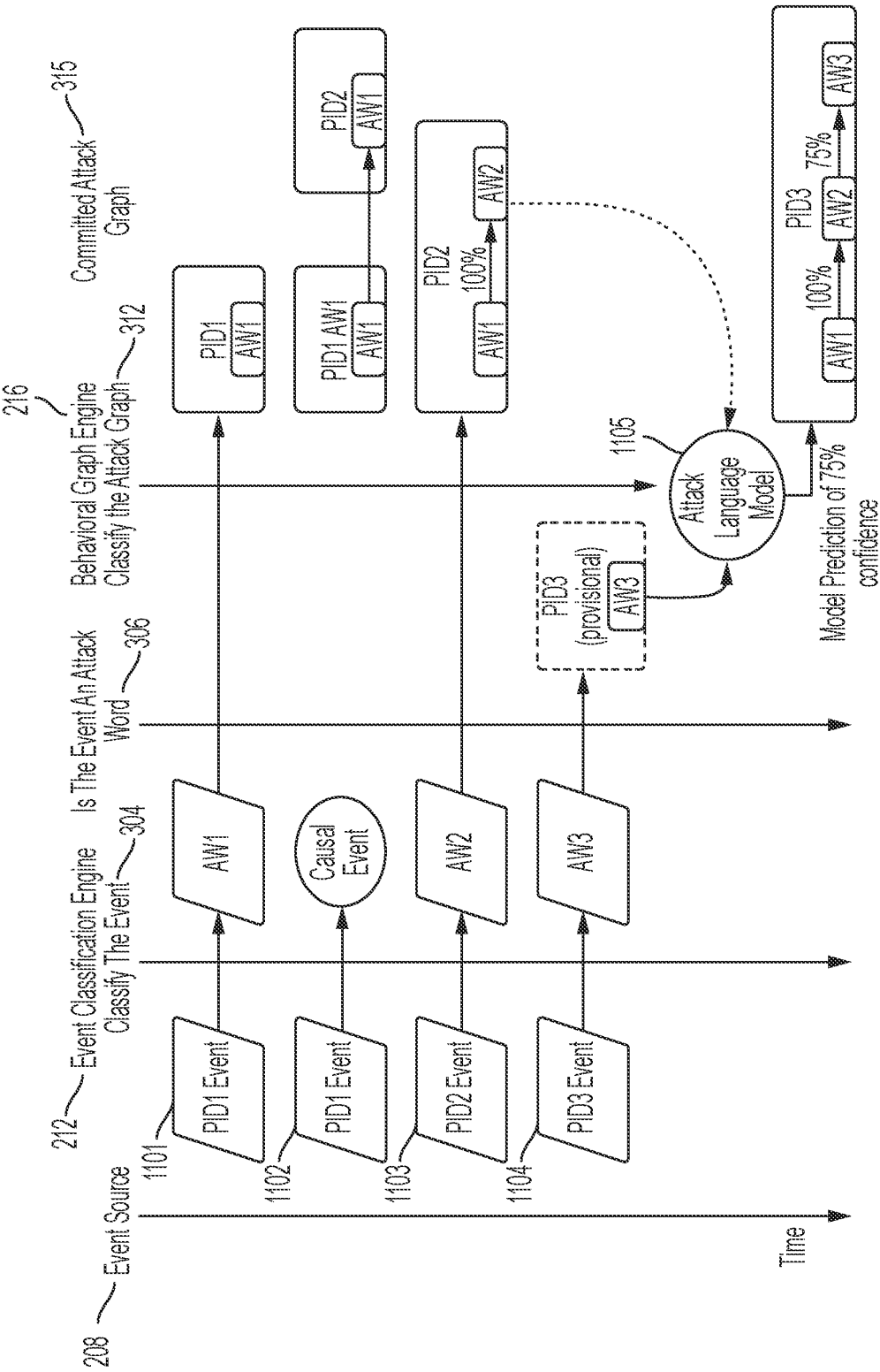


FIG. 12

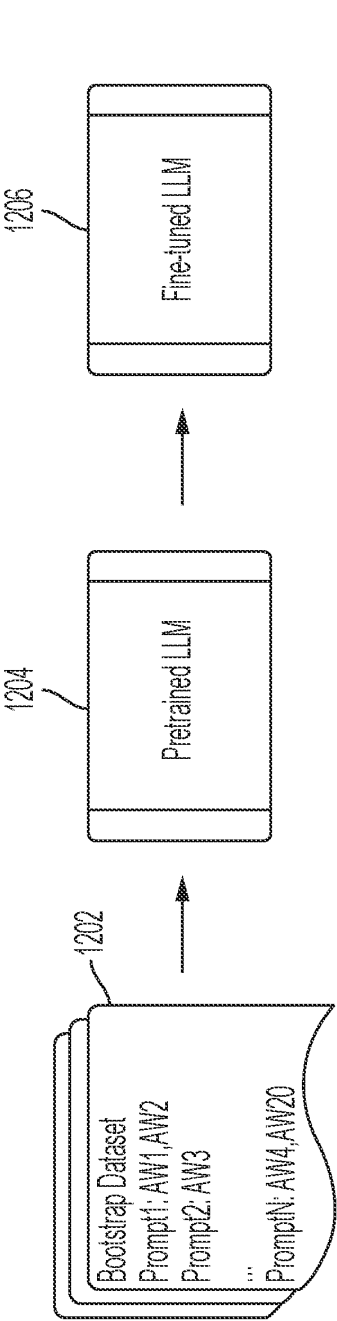


FIG. 13A

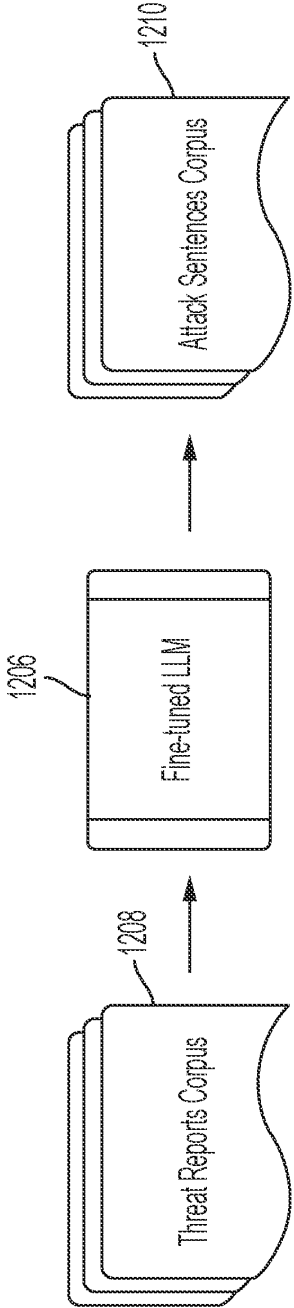


FIG. 13B

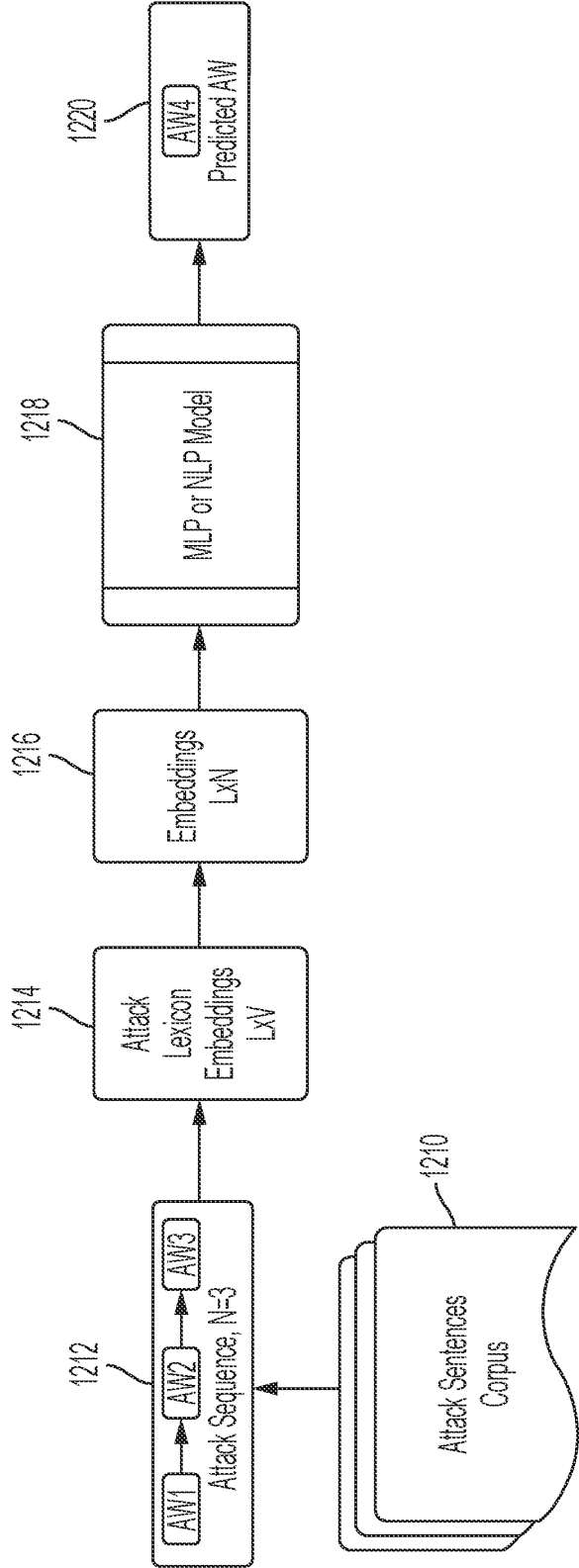


FIG. 14

```
rule label_MOTW:
{
  description:
    Label AW 1553.005 on files downloaded from the internet.

  reaction:
    Target.SetAttackWords(T1553.005)

  condition :
    (Op.Type == "FILE_CLOSE_MODIFIED") and
    (Target.FileZoneId >= 3)
}
rule label_DoubleExtension:
{
  description:
    Label AW T1036.007 - writing executable files with a double extension

  reaction:
    Target.SetAttackWords(T1036.007)

  condition:
    (Op.Type == "FILE_CREATE_NEW") &&
    ( Target.FileName == ["*.doc.???", "*.docx.???", "*.pdf.???", "*.xls.???", "*.xlsx.???", "*.sln.???",
    "*.png.???", "*.gif.???", "*.jpg.???", "*.jpeg.???", "*.avi.???", "*.mov.???", "*.mp3.???", "*.ppt.???", "*.pptx.???",
    "*.zip.???", "*.7z.???"] ) &&
    ( Target.FileExtension = [ "com", "exe", "bat", "cmd", "vbs", "vbe", "jse", "wsf", "wsh", "msc", "scr",
    "ocx", "sys", "pyw", "ps1" ] )
}

rule label_CredTheft:
{
  description:
    Label AW T1555.003 - processes reading MS Teams credentials
```

© 2023

FIG. 15A

reaction:

```
Initiator.SetAttackWords("T1555.003")
```

condition:

```
(Op.Type == "FILE_OPEN_READ") &&
```

```
(Initiator.Classification != "MSTeams") &&
```

```
(Target.FilePath == [
```

```
"<UserProfiles>\\*\\AppData\\Roaming\\Microsoft\\Teams\\Cookies",
```

```
"<UserProfiles>\\*\\AppData\\Roaming\\Microsoft\\Teams\\Local Storage\\leveldb\\*.log",
```

```
"<UserProfiles>\\*\\AppData\\Roaming\\Microsoft\\Teams\\Local Storage\\leveldb\\*.ldb" ])
```

© 2023

FIG. 15A
CONTINUED

```
rule evict_attackers:
{
  description:
    Terminate processes that more than 3 AW and the last one was predicted > 25% probability

  reaction:
    Evict, Log, Notify

  condition:
    (Initiator.AttackWords.Count > 3) &&
    (Initiator.NextAttackWordProbability > 25)
}
```

© 2023

FIG. 15B

```
rule causality_parent_to_child:
{
  description:
    Transfer state from parent to a newly created child proces

  reaction:
    Target.SetAttackWords(Initiator)

  condition:
    (Op.Type == "CREATE_PROCESS")
}
rule causality_file_to_process:
{
  description:
    Transfer state from parent to a newly created child proces

  reaction:
    Initiator.SetAttackWords(Target)

  condition:
    (Op.Type == ["LOAD_LIBRARY", "LOAD_SCRIPT"])
}
rule causality_process_to_file:
{
  description:
    Transfer state from a process to the newly written file

  reaction:
    Target.SetAttackWords(Initiator)

  condition:
    (Op.Type == "FILE_CLOSE_MODIFIED")
}
```

© 2023

FIG. 15C